IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION
Civil Action No: 3:08-CV-336

UBISOFT, INC. and UBISOFT ENTERTAINMENT, S.A., **Plaintiffs,** **v.** **OPTICAL EXPERTS MANUFACTURING, INC.,** **Defendant.**	**COMPLAINT**

Plaintiffs Ubisoft, Inc. and Ubisoft Entertainment, S.A. (collectively "Ubisoft" or "Plaintiffs") allege as follows:

NATURE OF THE ACTION

1. Ubisoft is one of the largest independent publishers and developers of video games in the world. One of its most successful games is *Assassin's Creed.* As a result of an extraordinary breach of trust and gross negligence by Defendant Optical Experts Manufacturing ("OEM"), one of OEM's employees leaked onto the worldwide web the PC version of *Assassin's Creed* (the "Game") six weeks prior to its release. This leak resulted in over 700,000 illegal, internet downloads of the Game, which caused Ubisoft to lose millions of dollars in sales. OEM should be held accountable for that loss.

JURISDICTION AND VENUE

2. This action arises under the United States Copyright Act, 17 U.S.C. §§ 101 et seq. Jurisdiction is based upon 28 U.S.C. §§ 1331 and 1338 and the principles of pendent

jurisdiction pursuant to 28 U.S.C. § 1367(a). This Court also has jurisdiction over the matter based on 28 U.S.C. § 1332(a)(1), because there is complete diversity between the parties, and the matter in controversy exceeds $75,000, exclusive of interests and costs.

3. Venue in this Judicial District is proper under 28 U.S.C. §§ 1391(b) in that a substantial part of the events giving rise to Plaintiffs' claims occurred in this Judicial District.

THE PARTIES

4. Plaintiff Ubisoft, Inc. is a California corporation , with its principal place of business in San Francisco, California.

5. Plaintiff Ubisoft Entertainment, S.A. is a French corporation, with its principal place of business in Montreuil, France.

6. Ubisoft is informed and believes, and on that basis alleges, that Defendant OEM is a North Carolina corporation, with its principal place of business in Charlotte, North Carolina.

FACTUAL ALLEGATIONS

The *Assassin's Creed* Videogame

7. Ubisoft is one of the world's largest videogame publishers and developers. Ubisoft publishes and develops videogames to be played on third-party videogame consoles such as the Sony PlayStation 3, the Microsoft XBOX 360 and the Nintendo Wii, as well as on PCs.

8. Ubisoft first released the videogame *Assassin's Creed* in November 2007 on the PlayStation 3 and XBOX 360 consoles. The game was enormously successful and quickly

proved to be one of Ubisoft's most valuable properties. Ubisoft released the PC version of *Assassin's Creed* on April 8, 2008. The *Assassin's Creed* videogame was developed by Ubisoft at its Montreal, Canada development studio.

9. Plaintiff Ubisoft Entertainment, S.A. is the owner of the exclusive rights and privileges in and to the copyright in the *Assassin's Creed* videogame, which is at issue in this lawsuit, and has a valid registration therein.

Ubisoft's Agreements With OEM

10. On September 18, 2007, Plaintiff Ubisoft, Inc. entered into a one-year written service contract with Defendant OEM to manufacture CDs and DVDs containing Ubisoft's videogames, which contract obligated OEM to "maintain the confidentiality of" and "not disclose" Ubisoft's Proprietary Information (the "Confidentiality Agreement").

11. In early to mid February 2008, in preparation for the worldwide release of the Game, Ubisoft contacted OEM and requested that OEM replicate copies of the Game to be used in testing the Game before release. Ubisoft was clear that the Game was highly confidential as it was not scheduled for worldwide release until April 8, 2008.

12. Ubisoft's director of security at its Montreal studio worked directly with OEM executives to determine the most secure method of transferring the Game to OEM for replication.

13. Prior to the transfer of the Game to OEM, Ubisoft requested orally and in writing that OEM follow "special" security measures while in possession of the Game because of the highly confidential and proprietary nature of the Game and because of the long period of

time that remained until release. These measures, included (1) appointing a single OEM representative to be Ubisoft's main contact person and to oversee the replication of the Game; (2) having that same OEM representative personally pack and account for the shipment of discs to Ubisoft; and (3) assuring that Ubisoft receive "every copy" of the Game that OEM created.

14. OEM represented orally and in writing that it understood the highly confidential nature of the Game and expressly agreed in an email sent to Ubisoft that it would follow the above security procedures. In reliance upon OEM's express representations that it would adhere to these "special," security measures, Ubisoft transferred the Game to OEM on February 22, 2008.

15. On February 25, 2008, OEM notified Ubisoft that the replication was almost complete. OEM shipped a package of ten Game discs to Ubisoft's Montreal studio later that same day. The sealed package was received the following day in Montreal and was opened by two Ubisoft employees, including Ubisoft's Montreal security director, who verified that the package contained ten discs from OEM. One of the discs was then used for testing the Game and kept under lock and key when not in use. The other nine discs were kept in a restricted, locked cabinet and were never used.

16. On or about February 29, 2008, Ubisoft discovered that a copy of the Game had been leaked onto the internet. Ubisoft was able to determine that the first server connections to the Game came from an address in North Carolina. Ubisoft is informed and believes, and on that basis alleges, that this address was the residence of an OEM employee.

17. Ubisoft was also able to determine that the copy of the Game that was leaked on the internet was the same copy of the Game that had been transferred from Ubisoft's Montreal

studio to OEM on February 22, 2008. The version of the Game that Ubisoft had transferred to OEM had a unique version number imbedded within it that was also appearing on the Game on the internet. Ubisoft had also placed a unique bug in the version of the Game transferred to OEM that was also appearing on the Game on the internet. It is common practice in the videogame industry to place a bug in pre-release games for security reasons, so if there is a leak the location of the leak can be more quickly identified.

OEM's Extraordinary Negligence and Breaches of Contract

18. On or about May 7, 2008, OEM met with Ubisoft in an effort to convince Ubisoft to continue using OEM for replication services (the "May 7 meeting"). During that meeting, representatives of OEM admitted to numerous breaches of the parties' express agreements regarding confidentiality, and to an extraordinary level of negligence that led directly to the leak of the Game.

19. During the May 7 meeting, OEM admitted that the OEM representative appointed to oversee the replication of the Game did *not* oversee the process. OEM confirmed that this employee did *not* even pack the discs that were sent to Ubisoft as had been explicitly requested by Ubisoft and agreed to by OEM. Nor did he personally account for the location of those discs. OEM also admitted that *no one* at the company kept track of the number of Game discs that OEM replicated or of what happened to those discs after they were created. To this day, OEM does not know how many discs of the Game were created, and cannot account for all of them.

20. In addition to disregarding Ubisoft's express security requests, OEM admitted at the May 7 meeting to having flagrantly disregarded its own security policies at the time of the

Assassin's Creed leak. OEM was supposed to have certain security policies in effect at the time of the leak. These included, but were not limited to the following:

(a) Material Pass Policy: The "Material Pass Policy" was designed to ensure that no OEM employees could leave OEM's facilities with customer property without having a "material pass," which detailed what material was being taken off-sight, whether the removal was approved by an authorized individual, and when, if ever, the material was due back. Upon exiting the building, a Security Manager was to inspect the items being removed, ensure they matched the quantity and description on the pass, check that the pass was signed by an authorized individual, determine if the items were to be returned to the facility, and file the pass so that it could be followed up on to determine if the appropriate materials were returned.

(b) Front Door Policy: The "Front Door Policy" was designed to "protect the intellectual property of OEM's customers" by ensuring that all OEM employees entered and exited OEM's building through an employee door. Visitors were to enter through the front door, but if they went beyond the executive offices and into the manufacturing facility, they too had to leave through the employee door. This employee door policy was critical to the security of OEM's facilities because it mandated that "Security will use a metal detector to screen everyone exiting the employee door." The Front Door Policy was designed to work in conjunction with the Exit Search Policy described below.

(c) Exit Search Policy: OEM's Exit Search Policy provided that "Loss Prevention Personnel are responsible for implementation of this procedure and for ensuring that exit searches, as described herein, are performed in a proper and consistent manner." Additionally, the Loss Prevention Manager was responsible for ensuring that all Loss

Prevention and Contract Security personnel were trained on the procedure, both at time of hire and every two months thereafter. The Exit Search Procedure then delineated a detailed procedure regarding how a Loss Prevention Manager was to conduct an exit search of any OEM employee leaving the premises.

21. During the May 7 meeting, OEM admitted that it was not following a single one of the above policies at the time of the *Assassin's Creed* leak.

22. Specifically, OEM admitted that it was not keeping track of the completed material passes. Accordingly, OEM had no way of knowing what materials were off-site at any given time, and/or whether they had ever been returned. Additionally, OEM's failure to trace Material Passes would have allowed a rogue OEM employee to modify an old pass without OEM's management ever knowing.

23. OEM admitted that Material Passes were readily available to any employee at all times. Indeed, the Material Pass forms were available on the J-drive of OEM's computer for any employee to print out. Thus, it was simple for any employee to forge a Material Pass in order to sneak a disc out of OEM's facilities.

24. OEM admitted that, at the time of the leak, OEM's security personnel were not regularly cross-checking the Material Passes with the material being taken off site by an employee. Therefore, as long as the employee held a Material Pass, he or she could have openly walked out with any disc in hand even if it was not the material described in the pass. OEM conceded at the May 7 meeting that this is what most likely occurred in the case of the *Assassin's Creed* leak.

25. OEM admitted that, at the time of the leak, its Loss Prevention personnel were *not* regularly searching exiting employees. Instead, OEM was using a "buddy system," whereby exiting employees searched each other before leaving the facility. The "buddy system" search procedure was in direct contravention of OEM's Front Door Policy and its Exit Search Policy, which *both* specifically provided that *Security* personnel would use a metal detector to screen everyone exiting the employee door.

26. OEM admitted that the metal detectors that were in place and being used by "buddy employees" at the time of the leak were incapable of distinguishing between common metal elements of clothing (such as a zipper, belt buckle or metal bra clasp) and a disc. OEM believes that any discs that were smuggled out of its facility were probably hidden in people's pants (so the beep from the metal detector would be blamed on a belt buckle or a zipper). While OEM agreed at the May 7 meeting that it would purchase new technology to allow OEM to determine the size of the metal object, so as to differentiate a disc from a zipper and allow for a meaningful search, OEM had *no* explanation whatsoever for why it was not using such metal detectors at the time of the *Assassin's Creed* leak.

27. OEM admitted that its failure to follow these policies (or the security measures it had expressly agreed with Ubisoft to follow with respect to the replication of the Game) had to be the cause of the leak because one of the OEM-manufactured Game discs had been found *off of OEM's premises*, at the residence of the OEM employee who had leaked the Game onto the internet.

28. In addition to the above security policies that were supposed to be in effect at the time of the leak but were *not*, OEM also had certain "facility controls" in effect at the time,

which were supposedly designed to ensure the security of the facility. Among those "facility controls" were extensive surveillance cameras, including 45 cameras inside and outside of OEM's manufacturing facility. Furthermore, the "masters" of proprietary client work were kept in a locked vault, to which only ten OEM employees had access. Finally, "waste discs" containing client materials were disposed of in locked containers and then destroyed under surveillance.

29. However, as Ubisoft discovered at the May 7 meeting, these "facility controls" were also seriously flawed. The 45 security cameras "guarding" OEM's facilities, including all exit doors, were not actually monitored by any security personnel or OEM employee. Instead, the cameras were simply recording videotape, only a random sample of which was viewed at a later date. While this random review may have allowed OEM to stumble upon a perpetrator after the fact, it did nothing to prevent a security breach from happening in the first place.

30. Additionally, OEM's policy that "master discs" of proprietary client work were kept in a locked vault to which few employees have access, and that any "waste discs" were disposed of in locked containers and destroyed under surveillance, were meaningless in practice. As noted above, OEM does not even keep track of the number of client discs that are made at its facility. OEM, for example, has no idea how many *Assassin's Creed* discs were made or whether they have all been located. Moreover, OEM admitted that "test" discs, which contain the most highly confidential intellectual property (because they generally contain material that has not yet been released to the public) were left in locked disposal containers for weeks, and that there were *no* security personnel overseeing their destruction. Instead, the discs were destroyed by an OEM employee who was being tape recorded but was not being monitored "live" by any other human being, and likely would never be seen at all.

31. As a result of the *Assassin's Creed* leak, OEM informed Ubisoft at the May 7 meeting that it would need to take steps to fix these egregious lapses in their security procedures in order to prevent any similar leaks from occurring in the future.

32. Given the above, it should have come as no surprise to OEM that the Game was leaked by one of its employees six weeks prior to its worldwide release.

FIRST CLAIM

Copyright Infringement

33. Plaintiff Ubisoft Entertainment, S.A. re-alleges and incorporates by this reference the allegations contained in paragraphs 1 through 32, inclusive, as though they were fully set forth herein.

34. Ubisoft Entertainment, S.A. is informed and believes, and on that basis alleges, that Defendant has infringed Ubisoft Entertainment S.A.'s copyright in the Game by, without limitation, copying, reproducing, distributing or otherwise exploiting the Game and/or by inducing, participating, causing or materially contributing to the foregoing.

35. Ubisoft Entertainment, S.A. is informed and believes, and based thereon alleges, that Defendant's infringing acts were committed willfully.

36. As a result of Defendant's copyright infringement as alleged above, Ubisoft Entertainment, S.A. has suffered and will continue to suffer injury and damage in an amount to be determined at trial. Furthermore, Ubisoft Entertainment, S.A. is informed and believes, and based thereon alleges, that Defendant has received or will receive profits, gains, or other benefits from its infringing activities, all of which should be disgorged to Ubisoft

Entertainment, S.A. In the alternative, Ubisoft Entertainment, S.A. reserves the right to seek statutory damages for Defendant's infringement of its copyright works.

37. Ubisoft Entertainment, S.A. has incurred and will incur attorneys' fees in pursuing this claim, which fees Ubisoft Entertainment, S.A. should recover from Defendant.

SECOND CLAIM

Breach of Contract

38. Ubisoft re-alleges and incorporates by this reference the allegations contained in paragraphs 1 through 32, inclusive, as though they were fully set forth herein.

39. OEM breached the Confidentiality Agreement by failing to comply with its obligation to "maintain the confidentiality of [Ubisoft's] Proprietary Information." OEM also breached the obligation that it "shall not disclose [Ubisoft's] Proprietary Information." OEM also breached its agreement by not following any of the "special," security requirements in connection with the Game and by materially departing from the terms of the bailment, which Ubisoft had specifically requested, and that OEM had expressly agreed to follow.

40. At all times relevant hereto, Ubisoft had fully performed all duties and obligations required of it by the parties' contracts, except as may have been excused or prevented by the acts or omissions of OEM.

41. As a result of OEM's breaches of contract, Ubisoft has been damaged by losing millions of dollars in lost sales in an amount to be proven at trial.

THIRD CLAIM

Negligence

42. Ubisoft re-alleges and incorporates by this reference the allegations contained in paragraphs 1 through 32, inclusive, as though they were fully set forth herein.

43. Ubisoft and OEM were in a relationship of bailor/bailee with regard to Ubisoft's intellectual property, *Assassin's Creed*. As a bailee, OEM had a legal duty to exercise ordinary care to protect the subject of the bailment, i.e. the Game, from harm. As the subject of the bailment was seriously damaged while in OEM's possession and control, Ubisoft is informed and believes, and on that basis alleges, that OEM breached its duty of care as bailee.

44. Ubisoft is informed and believes, and on that basis alleges, that OEM acted with gross negligence and breached its duty of care when it failed to follow any of its own security policies and procedures in connection with the Game, and when it implemented only "facial" facility controls that were useless to prevent the theft of its bailor's intellectual property. Indeed, Ubisoft is informed and believes, and on that basis alleges, that the minimal, facial "security" procedures that OEM actually had in effect at the time of the leak fell well below accepted standards in the replication industry. Ubisoft is informed and believes, and on that basis alleges, that the OEM employee's theft of the Game was the proximate result of OEM's breach of its duty of care as bailee.

45. As a direct and proximate result of OEM's negligence, Ubisoft has suffered millions of dollars in lost sales on the Game.

46. Ubisoft has also suffered serious and irreparable damage to its reputation. Many videogame websites and viewers have unfairly criticized the PC version of *Assassin's Creed* for

containing a bug that causes the Game to crash mid-way through. These critics and viewers are confusing the version of the Game that was leaked by OEM on the internet, and which intentionally contained a bug for security reasons, with the retail version of *Assassin's Creed* which does *not* have the bug.

47. Having this "broken" version of Ubisoft's highly anticipated Game on the internet weeks prior to its worldwide release was particularly harmful because reviews of the leaked version were mixed together with reviews of the retail version, creating confusion about whether there was a bug in the retail version of the Game. These negative reviews and publicity have further reduced Ubisoft's sales and caused irreparable harm to its reputation.

WHEREFORE, Ubisoft prays for judgment against Defendant as follows:

1. On Plaintiff Ubisoft Entertainment, S.A.'s First Claim for copyright infringement, for actual damages plus Defendant's profits in an amount to be determined at trial or, in the alternative, for statutory damages, plus Ubisoft's attorneys' fees;

2. On Ubisoft's Second Claim for breach of contract, for damages according to proof but in an amount in excess of $10 million, for costs of suit, for pre-judgment interest, and for such other relief as the Court may deem proper; and

3. On Ubisoft's Third Claim for negligence, for damages according to proof but in an amount in excess of $10 million, for costs of suit, for pre-judgment interest, and for such other relief as the Court may deem proper.

JURY DEMAND

Plaintiff demands a trial by jury.

This 16th day of July, 2008.

s/ Richard A. Vinroot
Richard A. Vinroot
N.C. Bar No. 4493
Pearlynn G. Houck
N.C. Bar No. 36364

ROBINSON, BRADSHAW & HINSON, P.A.
101 North Tryon Street, Suite 1900
Charlotte, NC 28246-1900
Telephone: (704) 377-2536
Facsimile: (704) 378-4000
rvinroot@rbh.com
phouck@rbh.com

Stephen S. Smith
California Bar No. 166539
Suann C. MacIsaac
California Bar No. 205659
Melissa A. Bakewell
California Bar No. 228715
GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 553-3610
Facsimile: (310) 553-0687
ssmith@greenbergglucker.com
smacisaac@greenbergglusker.com
mbakewell@greenbergglusker.com

Attorneys for Plaintiffs Ubisoft, Inc. and Ubisoft Entertainment, S.A.